# DISTRICT OF COLUMBIA JUSTIS SYSTEM
## USER ACCESS REGISTRATION/REQUEST FORM

Please specify the type of request this is by placing an "x" in the appropriate box next to the desired selection.

- ❏ Add new user
- ❏ Delete user

Requestor's First Name: _____M.I._____ Last Name: _____

Responsibility (e.g. Uniform Personnel, Criminal Justice Practitioner, Probation Officer,

etc.)_____

Position/Title: _____

Agency Name:_____

System User Training Certification Date:_____

System Security Awareness Training Certification Date: _____

Train the Trainer Certification Date: _____

New User – Please provide mothers' maiden name: _____

---

### Minimum Security Requirement for System Access

- ❏ NCIC Check
- ❏ Background investigation no more than 5 years old

**\*If NCIC is checked, user must sign NCIC release form**

---

### Agency Applications Request Section

Supervisor's/Manager's Signature: _____

Date: _____

Agency ITSO's Signature: _____

Date:_____

---

### JUSTIS Security Administrator's Section
Date Received:_____Date Processed:_____Processed By:_____

User id Assigned:_____

# ACKNOWLEDGEMENT OF JUSTIS ACCESS POLICY/USER AGREEMENT

I have read and understand the statements as they appear below.  As an authorized recipient of criminal history information, I understand that:

1) I must avoid any conflict of interest and/or any action that even appears to be fraudulent or negligent as it relates to accessing and disseminating criminal history information.
2) I shall not participate in the unauthorized processing or retrieval of information of a friend, enemy, neighbor, business associate, competitor or relative.
3) I shall not assist another employee in my office, another office, unit or division in unauthorized processing or retrieval of information of a friend, enemy, neighbor, business associate, competitor or relative.
4) I shall be responsible for the confidentiality of my network, as well as my application user identification numbers and passwords. At no time will I sign on to the system using another person's user identification number (s), and/or password (s), nor sign on to a terminal for the purpose of letting another individual use the system under my user identification number and password.  I will not share my Identification number and password with anyone.
5) I shall not vacate my terminal while connected to the network, system or application. I will sign off the system prior to leaving from eyesight of the terminal where I was signed-on.
6) I have been granted access to a government computer system and therefore acknowledge that JUSTIS data is government property and is to be used for official government business; I cannot release JUSTIS data for private use and I cannot sell it to anyone.
7) I have been trained in the use of the JUSTIS system for which I have been granted access and I have also been provided security awareness training.

I, (please print)_____ do hereby certify that I have read, understand, and have been given a copy of the above information.  I agree to abide by this policy and understand that non-compliance with any part may result in disciplinary action and/or criminal prosecution.

User's (Requestor's) signature: _____

Date Signed:_____

# JUSTIS RULES OF BEHAVIOR

The District of Columbia Intranet hereby known as JUSTIS may grant limited system access to certain contactors, clients and criminal justice practitioners who have demonstrated need to utilize the JUSTIS automated information resources.  However, as a condition of receiving this access, you are required to be aware of the JUSTIS system security policies and to abide by these policies.  This security policy emphasizes awareness practices for the purpose of safeguarding participating agencies' valuable information resources.

The system user identification (USERID) and password issued to you are your means to access these resources.  They are to be used solely in connection with the performance of your responsibilities as set fourth in your agreement with JUSTIS.  Use by anyone other than yourself is expressly prohibited.  You agree to be responsible for the confidentiality of the assigned information and accountable for all activity with your user identification (USERID).  Further, you agree that you will not provide this confidential USERID/password to another user nor will you sign on to the JUSTIS system so that another person may access or operate the workstation in your absence or on your behalf.  Actions of this type constitute a breach of system security and will result in immediate termination of your assigned USERID/password from the JUSTIS system.  In addition, you agree to:

a) Log-off the system when leaving the system/workstation area;
b) Refrain from leaving written passwords in the workstation area;
c) Avoid creating a personal password that can be easily associated with you;
d) Refrain from posting printouts of sensitive output data on bulletin boards;
e) Avoid leaving system output reports unattended or unsecured;
f) Avoid violation of the Privacy Act which requires confidentiality of personal data contained in government and federal and District of Columbia government data files;
g) Immediately contact your agency Information Technology Security Officer (ITSO) or the JUSTIS ITSO as appropriate, regarding any suspected violation or breach of system security;
h) Cooperate in providing personal background information to be used in conducting security background checks to the extent required by Federal regulations;
i) Respond to any inquiries and requests for information you may receive from either your agency ITSO, or the JUSTIS ITSO regarding system security practices.

CERTIFICATION: I have read the above statement of policy on Rules of Behavior regarding system security awareness and practices when assessing JUSTIS information resources.  I understand the JUSTIS policies as set forth above and I agree to comply with these requirements as a condition of being granted limited access to the JUSTIS computer resources.
User's (Requestor's) signature: _____
Date Signed:_____

JUSTIS ACCESS DESCRIPTION/POLICY

Prospective users will contact their agency Information Technology Security Officer (ITSO) to request access to JUSTIS. Agency ITSO's will be the single point of contact and act as the liaison between the user, the agency, and the JUSTIS ITSO organization. All agencies are required to have a security policy in place prior to that agency gaining access to JUSTIS. Agencies are also required to have an ITSO as well as an alternate ITSO. All users will complete a USER Access Registration/Request application prior to being scheduled for training. All users must receive JUSTIS practical application training and the security awareness training which will be provided by the appropriate JUSTIS ITSO organization member or agency trainer, prior to the user receiving access. All users should be encouraged by their agency ITSO to sign the RULES OF BEHAVIOR statement, which is to be kept on file by the ITSO at each user agency with a copy provided to the JUSTIS ITSO. All agency ITSO's will maintain a database of their users for audit purposes.

PROCEDURES FOR ACCESS:

1. The user will contact their agency ITSO to request access.
2. Users will complete a JUSTIS "User Access Registration Form". The agency ITSO will submit that application form to the JUSTIS ITSO.
3. The user will complete a JUSTIS "authorization for release of information" form enclosed in the JUSTIS application package provided by the agency ITSO. The agency ITSO will maintain this portion of the application at their respective agencies.
4. Agency ITSO's will schedule users for JUSTIS training after NCIC clearance is established.
5. Users will be trained by the appropriate agency ITSO or agency trainer.
6. Upon completion of training, ITSO's/trainers will forward user's access registration forms to the JUSTIS ITSO for processing.
7. The JUSTIS ITSO will accept a fax copy of the "User Access Registration/Request Form" as a temporary measure until the original application is received via mail or courier, provided that the ITSO signature is that of a recognized and viable agency ITSO organization member.
8. The JUSTIS ITSO will provide the user with a JUSTIS user identification number/password via the appropriate agency ITSO.
9. The JUSTIS ITSO will maintain an electronic database of all agency ITSO's and JUSTIS users as well as identification numbers/passwords issued.

## DISTRICT OF COLUMBIA                    JUSTIS SYSTEM

### AUTHORIZATION FOR RELEASE OF INFORMATION
### NCIC  (National Crime Information Center) CHECK

I hereby authorize a representative of the_____(agency name) to obtain any information on me while conducting a criminal history background check.  I understand that this check must be done before I am allowed to access the JUSTIS system.  I also understand that refusal to provide all necessary information may result in, 1) denial of access to JUSTIS and, 2) denial of access to JUSTIS data.

1.  Name (Last, First, Middle)

2.  Address (Street address)  (City,  State, County, Zip code)

3.  Home Telephone Number (Area Code, Number):

4.  Aliases/Nicknames:

5.  Citizenship (List the country you are a citizen of):

6.  Social Security Number:

7.  Date of Birth (Month, day, year):

8. Sex:                    Race:                    Height:                    Weight:

9. Eye Color:                          Hair Color:

10. Place of Birth (City, State, Country)

11.The above listed information is true and correct. Applicant's signature   12. Date

*PRIVACY ACT NOTICE*

**Authority for Collecting Information:** E.O.10450; 5 USC 2165 and 2455; USC 2585 and 2519; and 5 USC 3301

**Purposes and Uses**: Information provided on this form will be furnished to individuals in order to obtain information regarding activities in connection with an investigation to determine fitness/clearance for system access. The information obtained may be furnished to third parties as necessary in the fulfillment of official responsibilities.

**Effects of Non-disclosures**: Furnishing the requested information is voluntary, but failure to provide all or part of the information may result in a lack of further consideration for access or in the termination of existing access.